The flag byte is at the beginning of each frame, and is used to indicate the start of the frame. The address byte is used to distinguish commands from responses (for point-to-point lines). The control byte is used primarily for sequence numbers and to distinguish the different types of frames. The information field is used for arbitrary information and may be arbitrarily long (length is actually limited by the effectiveness of the Cyclic Redundancy Check (CRC)). The CRC bytes are used for frame error detection.

4.2.2.3.2.1 Modified LAPB

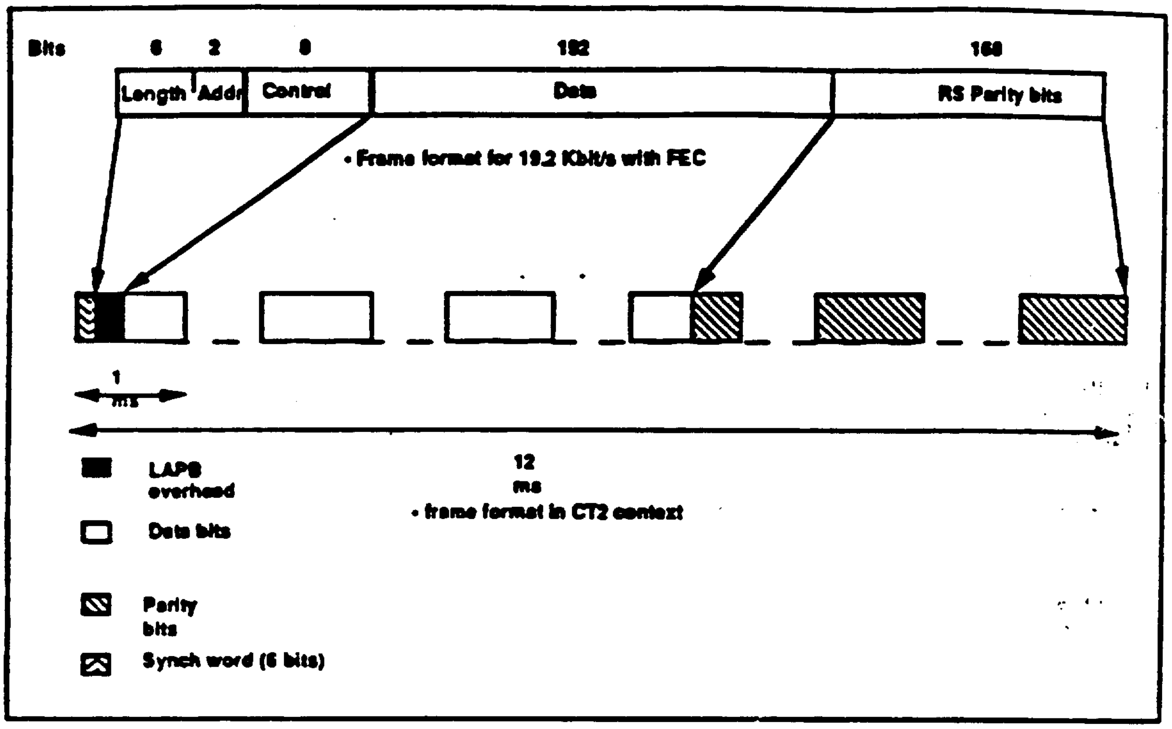
The LAPB frame is to be inserted in a number of transmit bursts. A synchronization word (6 bits) is used at the beginning of the frame to establish which burst is first in the frame. Thus, by sharing PCI framing, the LAPB flag bytes and zero bit stuffing can be eliminated. The ARQ frame length information must be added to the frame header, which can be multiplexed into the address byte of LAPB. The length information is six bits long, which is sufficient to cover the maximum length of data in a LAPB frame. The elimination of the flag bytes and zero bit stuffing results in an increased number of available bits that are used by the FEC code. The data field is a multiple of 8, since it will contain a certain number of eight bit characters. When there is not enough data to fill the maximum data field available, then arbitrary information is used for filling. The CRC bytes are also eliminated, since RS codes already provide for error detection capability. The resulting frame is shown in Fig. 4.5, where I is the number of eight-bit characters to be transmitted.

Figure 4.5 Modified LAPB frame

Bits	6	2	8	8*I
	Length	Addr	Control	Data

The modified LAPB frame is aligned with the Multiplex 1 burst structure (CAIS, part 2, Figure 2.2). Multiplex 1 supports 64 B channel bits. Six bursts are used to carry a complete LAPB frame plus the FEC parity bits (see Fig. 4.6).

Figure 4.6 Frame Format .in PCI Context



In order to provide the maximum desired throughput of 19.2 kbit/s, we need at least 192 bits out of the 384 bits provided by six transmit bursts. The PAD strips the start, stop and parity bits so the asynchronous rate of 19.2 kbit/s translates to a 15.36 kbit/s synchronous rate over the air interface (19.2 * 8/10= 15.36). This corresponds to 184.32 bits for a 12 ms frame. However, since we restrict the LAPB data field to be a multiple of 8 we actually need 192 bits. Adding the bits required by the length+address and control bytes we get:

192+8+8 = 208 bits

If we use an RS code with 6 bits per symbol, then the maximum block length we can use is 63 symbols or 378 bits. The resulting RS code is (378/6,208/6)=(63,35;1) with 1 parity symbol reserved for error detection. Also, the LAPB timeouts have to be customized for the PCI network implementation.

4.2.2.3.3 Multimode FEC

In the case of the lower rates (eg. 9600 bit/s, 4800 bit/s etc.) it is advantageous to use a different more powerful FEC code, that would utilize the extra available capacity. This would provide better error protection and consequently it would improve the throughput. Experimental results of using this method have been demonstrated for 9600 bit/s[6].

Therefore, a multimode FEC technique is used, where the FEC code used is determined by the maximum bit rate provided by the user. Table 4.1 lists the resulting RS codes.

Table 4.1 Multimode FEC

Mode	Rate (bit/s)	RS code (n,k;d)
1	300	(63,4;1)
2	1200	(63,6;1)
3	2400	(63,7;1)
4	4800	(63,11;1)
5	9600	(63,19;1)
6	14400	(63,27;1)
7	19200	(63,35;1)

4.3 Transparent Data Service

The transparent data service provides the user with an unrestricted access to the 32 kbit/s B channel, or to subrate channels. Data rates are synchronous and user selectable. The supported rates are: 300, 1200, 2400, 4800, 9600, 14400, 19200 and 32,000 bit/s. The service has the capability of providing FEC for all rates except 32 kbit/s, at the user's request. Reed Solomon (RS) codes are used for FEC similar to the asynchronous data service. However, there is no ARQ protocol, and there is no guarantee of data integrity.

4.4 X.25 Packet Data Service

This service allows terminals with X.25[7] capabilities to communicate with private or public landline packet data networks (Fig. 4.7).

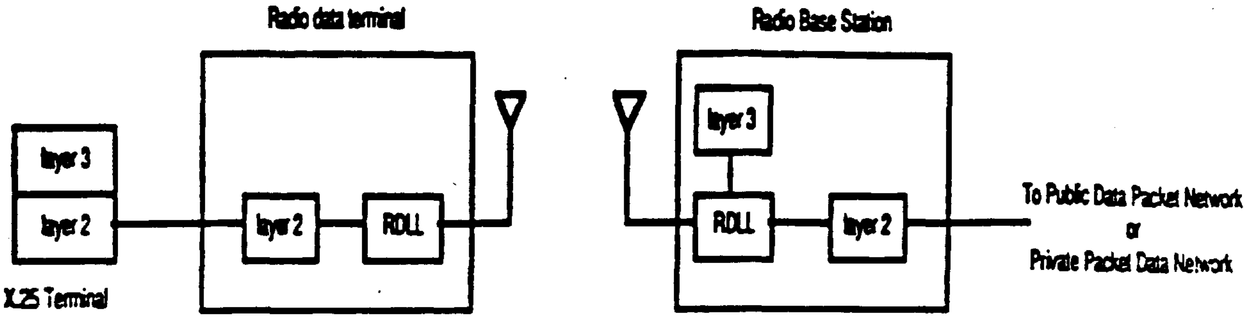
In Fig. 4.7, the X.25 layer 2 at the portable data terminal communicates with the X.25 layer 2 of the X.25 terminal. The data is then given to the RDLL for transmission over the radio link. At the Base station and Network controller, the RDLL (a) passes the data to an X.25 layer 2 for transmission over a landline packet data network or (b) distributes the data locally. In the

[6] G. Mony, J. Michaelides, B. Topis, Asynchronous Data Transport on Digital Cellular Radio, Worldwide Personal Communications Comforum, June 1990.

[7] The International Telegraph and Telephone Consultive Committee. "Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit." Recommendation X.25, Malaga-Torremolinos, 1984

second case, an X.25 layer 3 is implemented at the Base station and Network Controller for communicating with the X.25 terminal's layer 3.

Figure 4.7 X.25 Packet Data Service



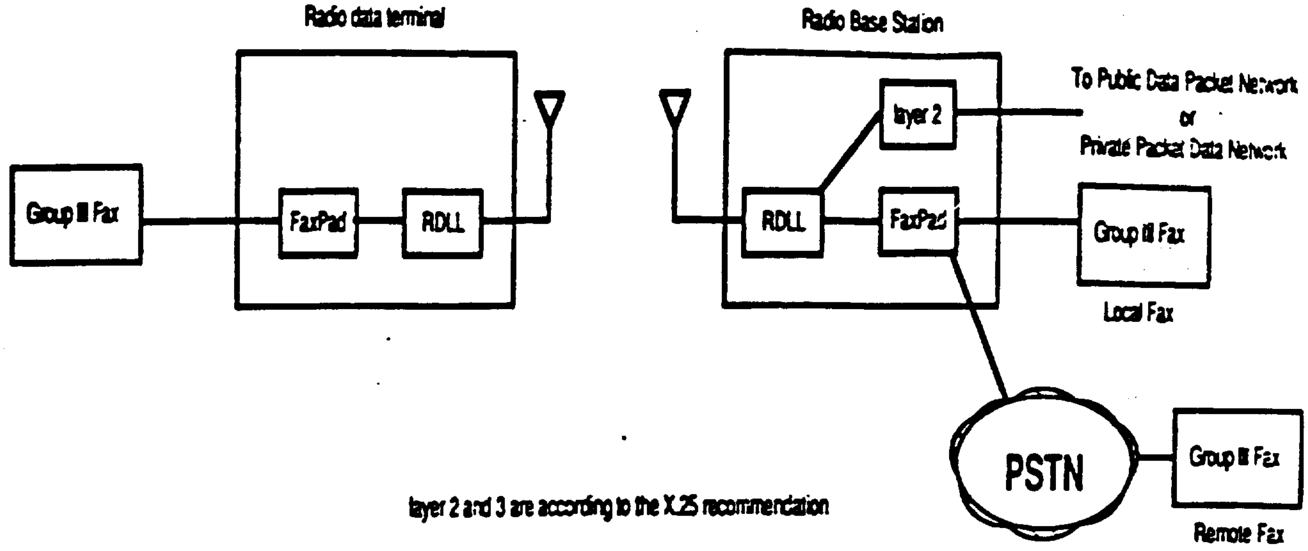
layer 2 and 3 are according to the X.25 recommendation

An asynchronous terminal can also communicate over a landline packet data network by accessing a PAD using the asynchronous data capability of the PCI system, as described in section 4.2.

4.5 Group III Fax Service

The PCI system supports the transmission and reception of G3 Fax messages. A G3 Fax machine is connected to the PCI data terminal via an analog or digital interface (Fig. 4.8). A FaxPad is used as an interface between the fax protocol and the radio transport. The FaxPad provides for appropriate mechanisms in order to communicate with a G3 Fax machine and to receive the user data. It also provides for the exchange of control information between FaxPads. It assembles/disassembles the user data and control information into/from packets, using datafields defined in the X.25 recommendation (packet level). The FaxPad uses the RDLL as its layer 2.

Figure 4.8 G3 Fax Service



A G3 Fax machine connected to a PCI data terminal may access a G3 Fax machine (a) over a landline packet data network or (b) through a circuit switched connection. In the first case, the FaxPad located at the PCI data terminal communicates with a corresponding Faxpad located within the landline packet data network. This case allows G3 Fax machines connected to PCI data terminals to access G3 Fax machines that use a packet data network to transmit or receive their messages. In the second case, the FaxPad located at the PCI data terminal communicates with the FaxPad located at the Base station and Network controller for a circuit switched connection to a local G3 Fax machine, or to a G3 Fax machine connected to the Public Switched Telephone Network (PSTN).

In case the FaxPad is implemented within the G3 Fax machine, then this Fax machine may use the X.25 packet data service (as described in section 4.4) for the transmission/reception of Fax messages.

Currently, the CCITT is in the process of examining recommendations X.5, X.38 and X.39, which specify a FaxPad that would provide connection of G3 Fax machines through packet data networks. These recommendations could be used for the implementation of the FaxPad shown in Fig. 4.8.

The RDLL is the same as specified for the asynchronous data service.

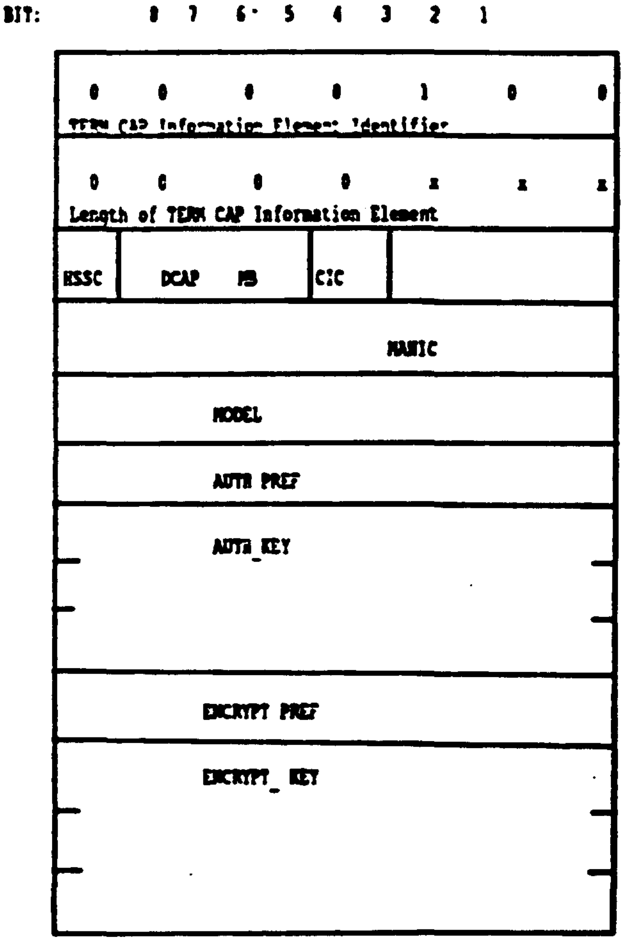
5. Security

Cryptographic techniques can provide both privacy and authentication. Annex C of the CT2 CAIS specifies the mechanisms of basic authentication to be used in PCI handsets.

5.1 Layer 3 Information Elements

5.1.1 Terminal Capabilities Information Element

Encryption for calls is offered as an option in the PCI system. The option is invoked via the Terminal Capabilities Information Element (TERM_CAP). This information element is described in the CAIS Signalling Layer 3, Section 2.2.10. Additional fields are added to the Terminal Capabilities Information Element to support encryption.



Encrypt_Pref is used by the CPP to indicate to a CFP which of the encryption algorithms offered by the CPP is the CPP's preferred algorithm. If only one algorithm is offered, this must be indicated as the preferred algorithm in this field.

Encrypt_Key is a bit field used to indicate to a CFP which encryption algorithms the CPP is capable of performing. A bit if set to 1 indicates that the CPP is capable of performing the associated algorithm, and if the bit is set to 0 the CPP is not capable of performing the associated algorithm.

5.1.2 Alternative Encryption Request Information Element (ENCRYPT2_REQ).

This alternative encryption request information element is used by a CFP to initiate the alternative call encryption process.

BIT: 8 7 6 5 4 3 2 1

0 x x x x x x x ENCRYPT2 REQ Information Element Identifier
Length of ENCRYPT2 REQ Information Element
ENCRYPT NO

ENCRYPT_NO is used to indicate to the CPP which (if any) of the encryption algorithms offered by the CPP is to be used.

5.2 Mutual Authentication & Encryption Key Generation

The voice/data channel (B channel) is encrypted using a private key cryptosystem. The private key cryptosystem could be based on the encryption function "F" used for Telepoint authentication. Two private keys are used (one for each direction of transmission). The private keys are derived by extending the telepoint authentication procedure (CAIS, Annex C). A new pair of encryption keys is generated for each session or call.

A handset contains identification information which is transmitted to the CFP during the setup and authentication phases of a call. This information is sufficient to uniquely identify the handset. The handset also stores internally a PIN number which is transmitted to the base station during the setup and authentication phases of a call.

To avoid problems of fraud (arising from the monitoring of the air-interface and the cloning of valid handsets) the PIN is encrypted before transmission over the air-interface.

The process by which the content of the PIN field is interrogated by the base and the handset authenticated is:

-The base transmits to the handset a 32-bit random challenge (RAND1) in the Layer 3 Information Element AUTH_REQ where it is received as RAND1'.

-The handset encrypts the 64-bit PIN using an encryption function "F", and using RAND1' as the key to produce the the 32-bit cyphered-PIN (CPIN1).

-The handset then transmits CPIN1 to the base in Layer 3 Information Element AUTH_RES where it is received as CPIN1'.

-The base determines the expected-PIN (E-PIN1) for the handset using the Identification Information and using the same function "F", with RAND1 as the key, calculates the expected value of CPIN1 (E-PIN1).

-The base compares the received CPIN1 (CPIN1') with the expected value (E-PIN1). If the values match the handset is judged to be valid.

A similar process can be used to authenticate the base to the handset:

-The handset transmits to the base a 32-bit random challenge (RAND2) in the Layer 3 Information Element AUTH_REQ where it is received as RAND2'.

-The base encrypts the 64-bit PIN using an encryption function "F", and using 'RAND2' as the key to produce the the 32-bit cyphered-PIN (CPIN2).

-The base then transmits CPIN2 to the handset in Layer 3 Information Element AUTH_RES where it is received as CPIN2'.

-The handset encrypts the 64-bit PIN using the same function "F", with RAND2 as the key, calculates the expected value of CPIN2 (E-PIN2).

-The handset compares the received CPIN2 (CPIN2') with the expected value (E-PIN2). If the values match the base is judged to be valid.

The process by which the encryption key (Key_P_to_F) for the CPP to CFP link is obtained is:

-the handset and base each encrypt the 64-bit PIN using the encryption function "F" and using CPIN1 as the key to produce the 32-bit cyphered CPIN1 (C-CPIN1).

Key_P_to_F = C-CPIN1.

The process by which the encryption key (Key_F_to_P) for the CFP to CPP link is obtained is:

-the handset and the base each encrypt the 64-bit PIN using the encryption function "F" and using CPIN2 as the key to produce the 32-bit cyphered CPIN (C-CPIN2).

Key_F_to_P = C-CPIN2.

The method can be easily generalized to generate 64-bit keys if required.

The sections above have assumed that the base station, given the identity of the handset (and account), will know the value of the PIN expected from the handset (E-PIN).

6. Half-Slot Channels

The provision for half-slot channels will allow PCI to take advantage of future low bit rate speech coders and/or more efficient modulation schemes. A number of different frame structures are possible. One option, presented in Fig. 6.1, would allow the use of 2-channel TDMA on each standard 2 ms frame. Radios using the half-slots would still have to meet the channel spectral mask and power levels; thus, they would cause no more interference than standard full-slot transmitters.

Figure 6.1: Frame Structure for Half-Slot Channels

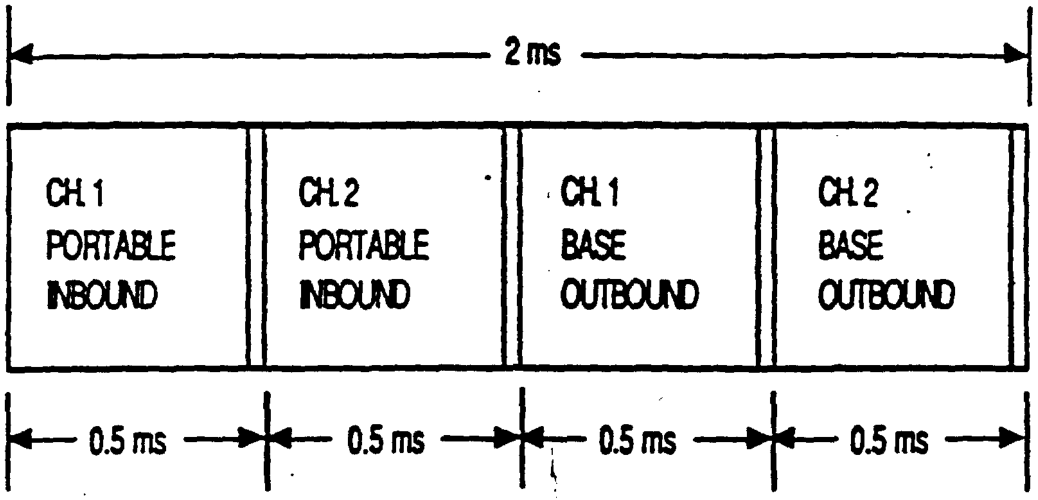


EXHIBIT F

PCI

Personal Communications Interface

- Why PCI
- What is PCI
- Advantages of PCI

EXHIBIT F

Why PCI

Requirements in the work place, residence, public area for:

- mobility / reachability
- lower installation, maintenance and re-wiring costs
- quality
- capacity
- privacy

Need to operate in available spectrum

Need for coexistence of applications and service / product suppliers

- availability of Common Air Interface standard
- availability of equipment from many suppliers

Opportunity for service providers to take lead in offering PCS

- learn and prove market requirements
- develop network support for mobility: roaming, hand-over, billing

Demonstrate need for spectrum allocation for expanded service

Customer demand for wireless services NOW

Evolution

Dedicated (primary) spectrum (CCIR: 60-120 MHz)

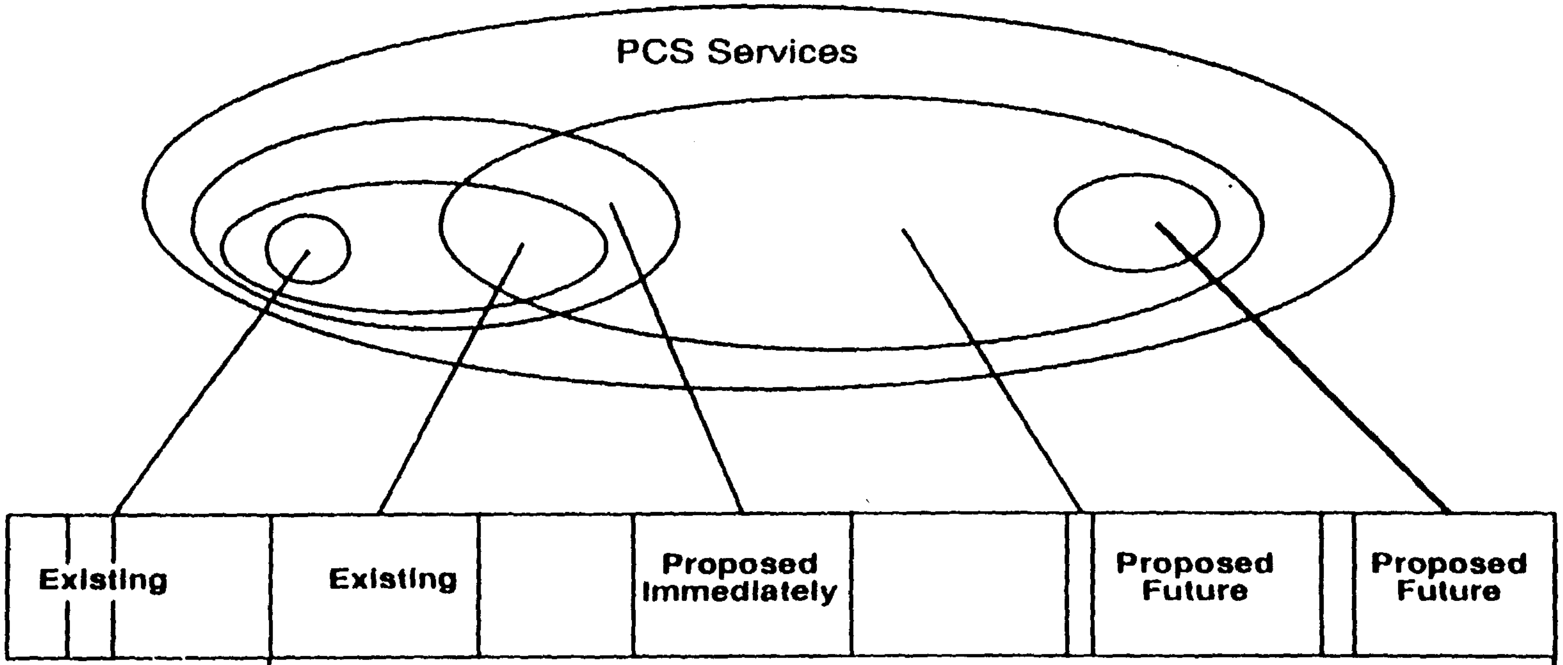
Personal Communication Services

- integrated with PSTN / ISDN
- wide area applications
- universal access
- higher capacity

Build on network services and market demand established

PCS Service & Spectrum Relationships

BNR



PCS Services

Existing

Existing

Proposed Immediately

Proposed Future

Proposed Future

49 MHz
- Low Density
- Cordless Telephones

800 MHz
- Mobile Cellular

900 MHz
- Personal Communications Services Phase I
  - Low Power
  - In Building / In Transit
  - Common Mobile Terminal/Numbers

1.7 GHz   2.3 GHz

Immediate - Trials
Future Phase 2 Service
- Contiguous Service
- Picocell / Microcell / Macrocells
- Service Expansion
- FPLMTS

230 MHz min.*

LM446007 b/w

* Includes Mobile Cellular

What is PCI

BNR

PCI is Northern Telecom's proposal for an open standard in North America

- Proposed in Northern Telecom response to FCC NOI on PCS
- Addresses the non-availability of primary spectrum
- Proposes approach that still offers opportunity of North American roaming
- Utilizes available primary spectrum (930-931 MHz and 940-941 MHz) and provides for sharing of secondary spectrum (930-960 MHz)
- Builds on and offers full compatibility with the CT2Plus standard already proposed in Canada
- Changes to planned CT2Plus are minor

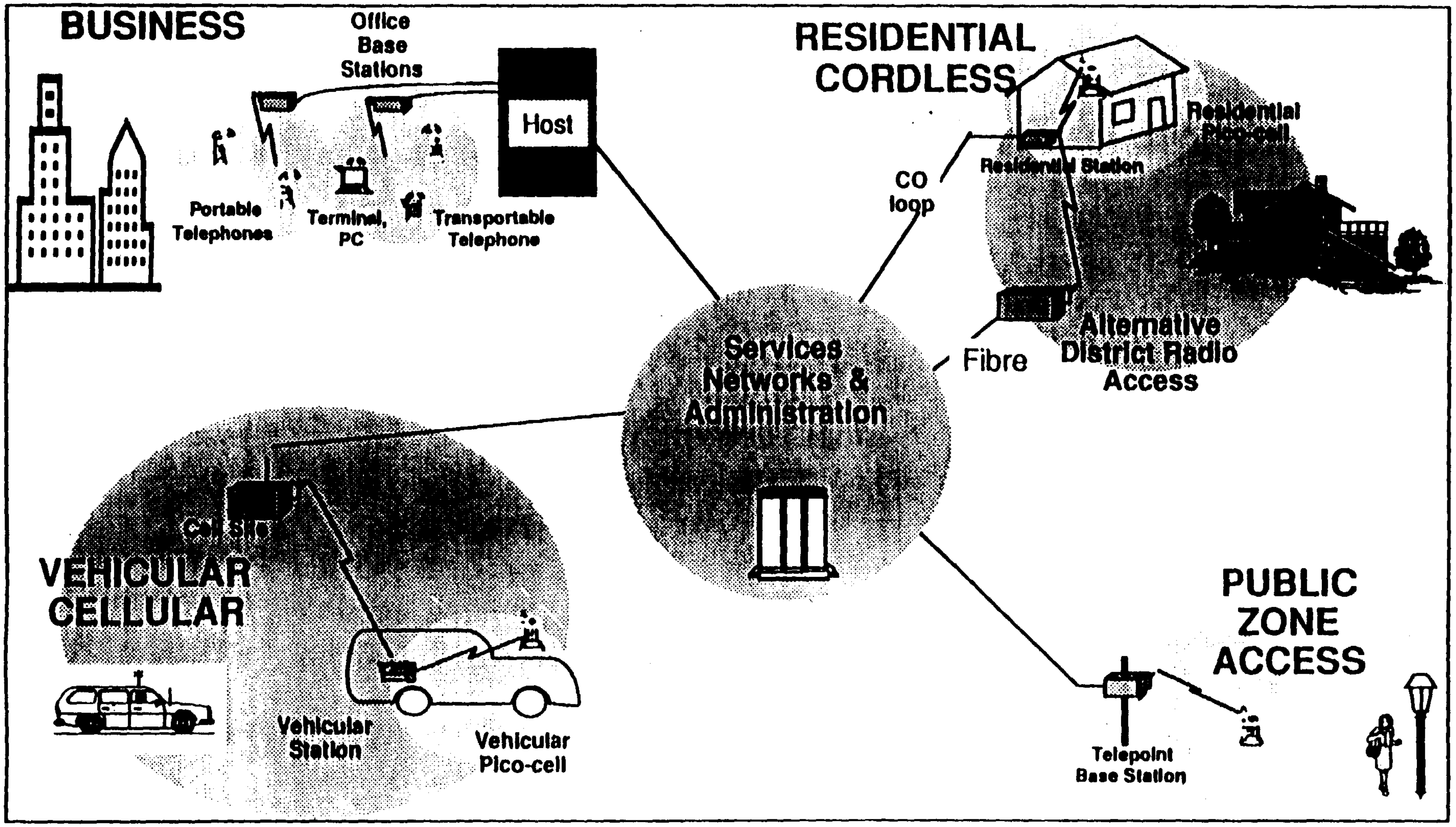
  (channel management control for shared spectrum & frequency agility in US)

PCI is unique in offering the opportunity of an immediate North American compatible service.

PCI consists of:

- CT2 Common Air Interface specification (MPT1375)
- with enhancements and modifications to meet North-American requirements and spectrum availability

PCI Comprehensive Applications



Pocket Telephone
+
Organizer & Personality

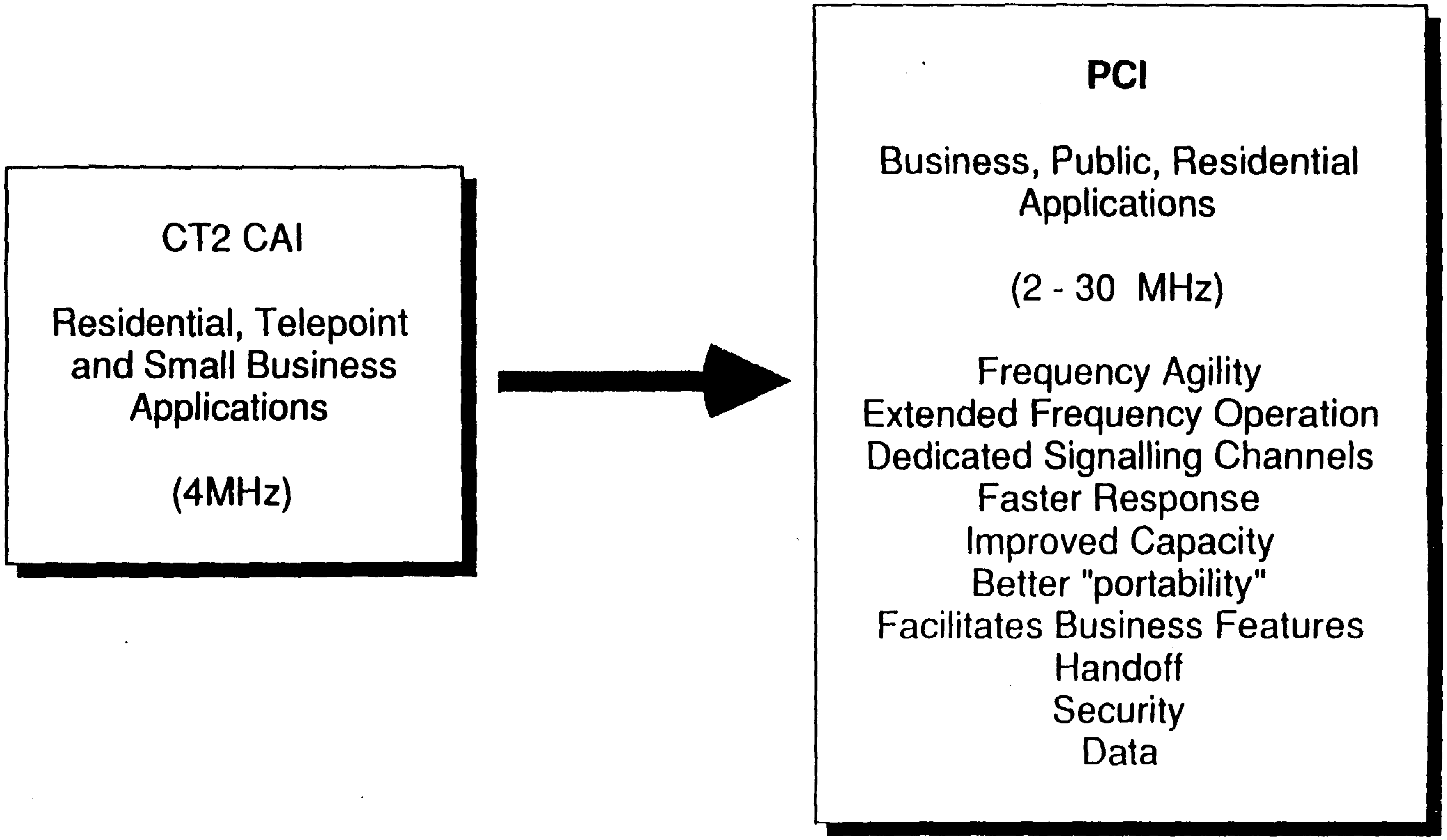
→

Personal Communication
& Transaction Device

→

New Services
& Revenues

Key PCI Enhancements



CT2 CAI

Residential, Telepoint and Small Business Applications

(4MHz)

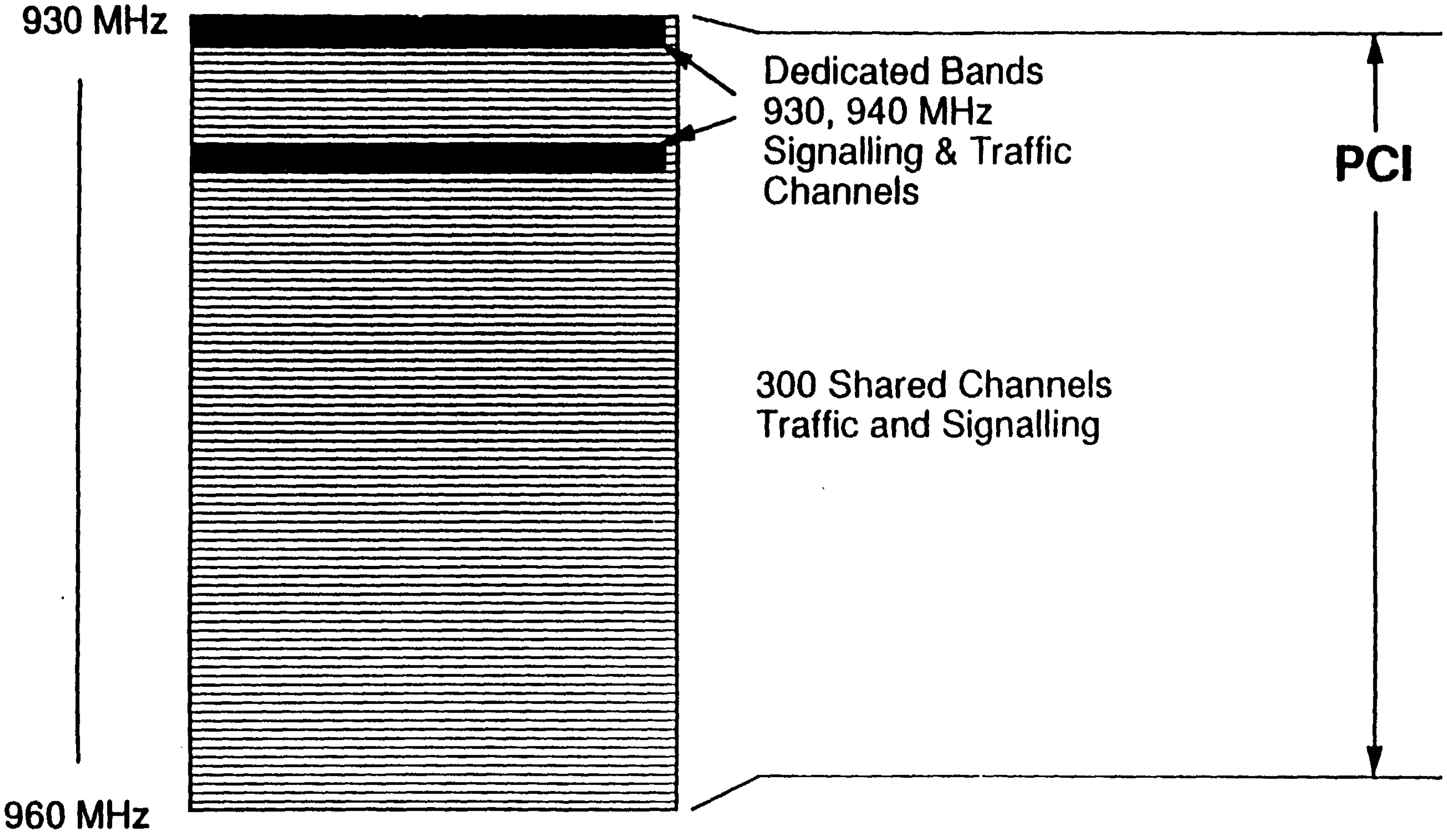
PCI

Business, Public, Residential Applications

(2 - 30 MHz)

Frequency Agility
Extended Frequency Operation
Dedicated Signalling Channels
Faster Response
Improved Capacity
Better "portability"
Facilitates Business Features
Handoff
Security
Data

Spectrum for PCI



930 MHz

960 MHz

Dedicated Bands
930, 940 MHz
Signalling & Traffic
Channels

300 Shared Channels
Traffic and Signalling

PCI

PCI Radio Characteristics

Common Air Interface

Single Band Operation (transmit-receive)
- via Time-Division-Duplexing
- only one RF front-end filter required
- reciprocity gives diversity gain in both directions with antennae only at base station

Dynamic Channel Allocation
- Everyone shares the entire low-power wireless band
- More bandwidth available to each user
- Allows uncoordinated adjacent systems to coexist
- More flexibility and less RF propagation engineering required to plan cell sites

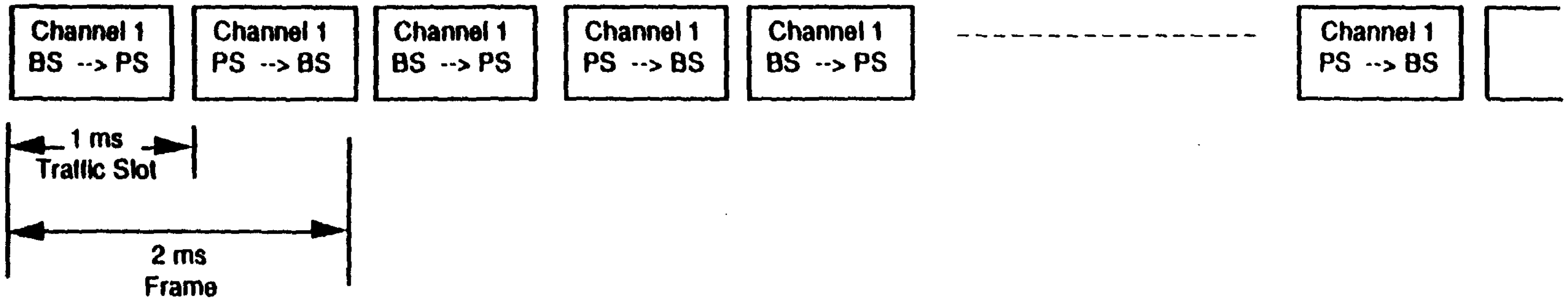
100 kHz Channels

10 mw Power

Low Delay

PCI Frame Formats

CT2 - PCI Traffic Frame Structure



Channel 1 BS --> PS

Channel 1 PS --> BS

Channel 1 BS --> PS

Channel 1 PS --> BS

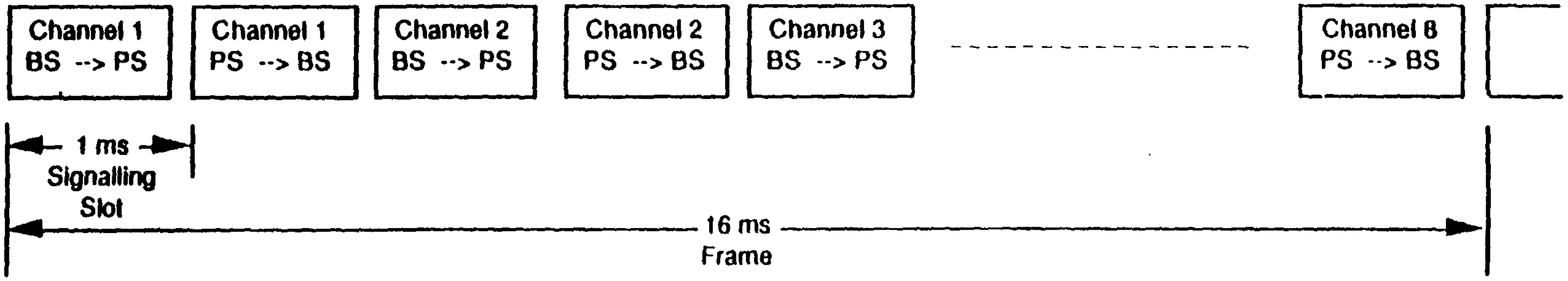
Channel 1 BS --> PS

Channel 1 PS --> BS

1 ms Traffic Slot

2 ms Frame

PCI Signalling Frame Structure



Channel 1 BS --> PS

Channel 1 PS --> BS

Channel 2 BS --> PS

Channel 2 PS --> BS

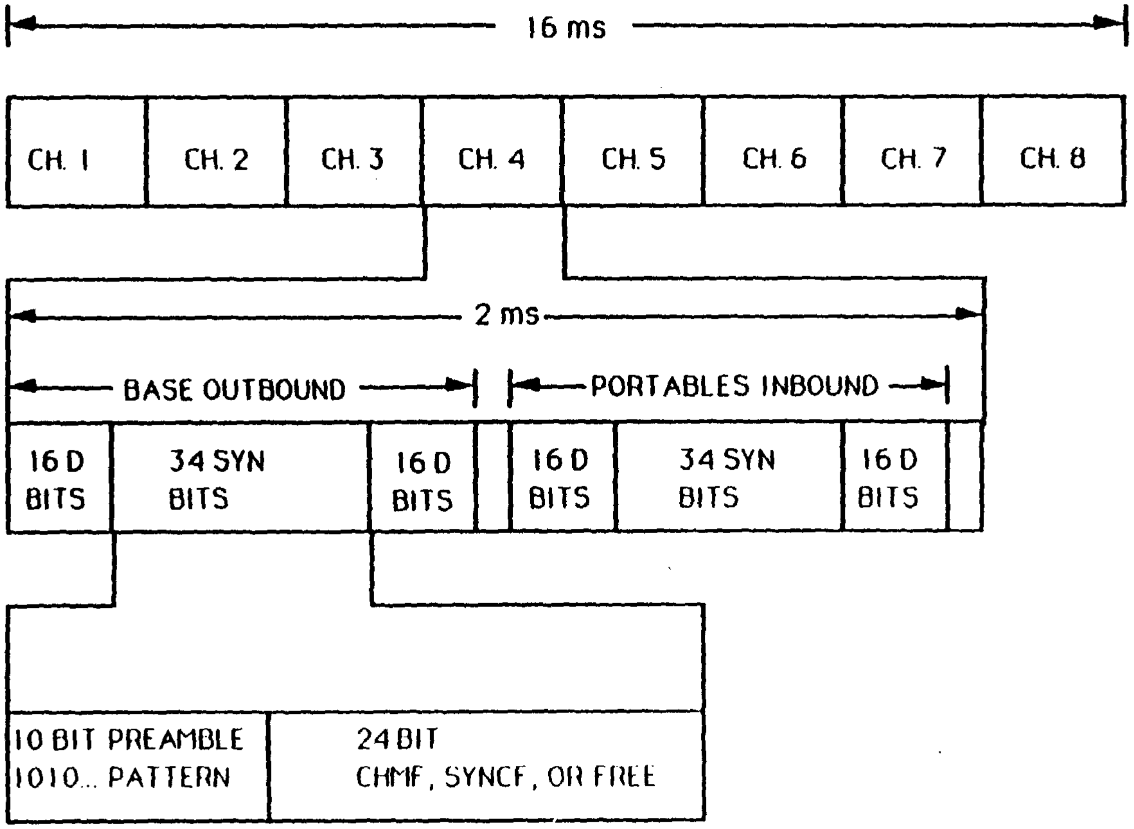
Channel 3 BS --> PS

Channel 8 PS --> BS

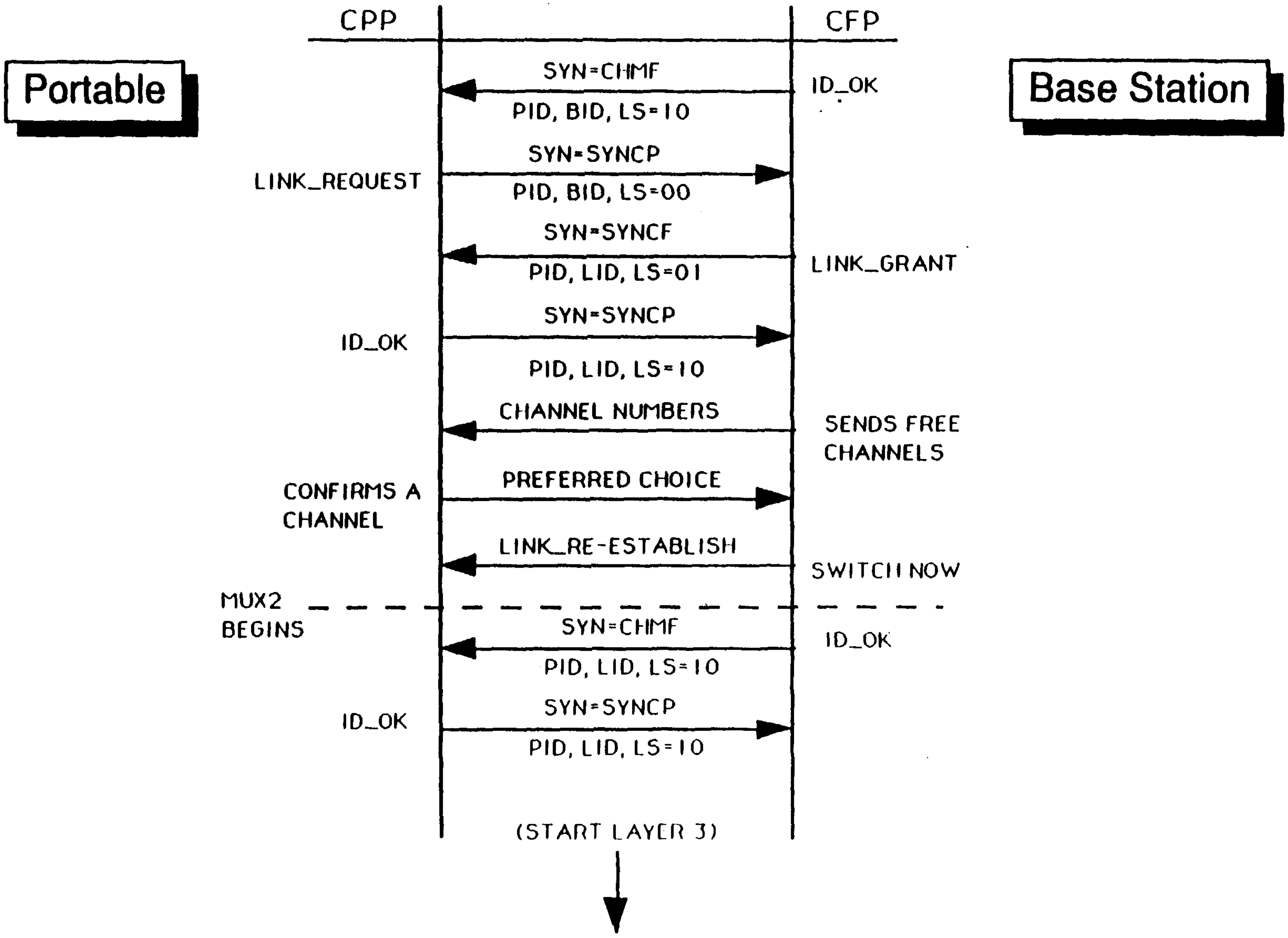
1 ms Signalling Slot

16 ms Frame

PCI Radio Control & Signalling Channels



PCI Call Set-up Using Control Channel



Portable

Base Station

CPP

CFP

SYN=CHMF

ID_OK

PID, BID, LS=10

SYN=SYNCP

LINK_REQUEST

PID, BID, LS=00

SYN=SYNCF

LINK_GRANT

PID, LID, LS=01

SYN=SYNCP

ID_OK

PID, LID, LS=10

CHANNEL NUMBERS

SENDS FREE CHANNELS

PREFERRED CHOICE

CONFIRMS A CHANNEL

LINK_RE-ESTABLISH

SWITCH NOW

MUX2 BEGINS

SYN=CHMF

ID_OK

PID, LID, LS=10

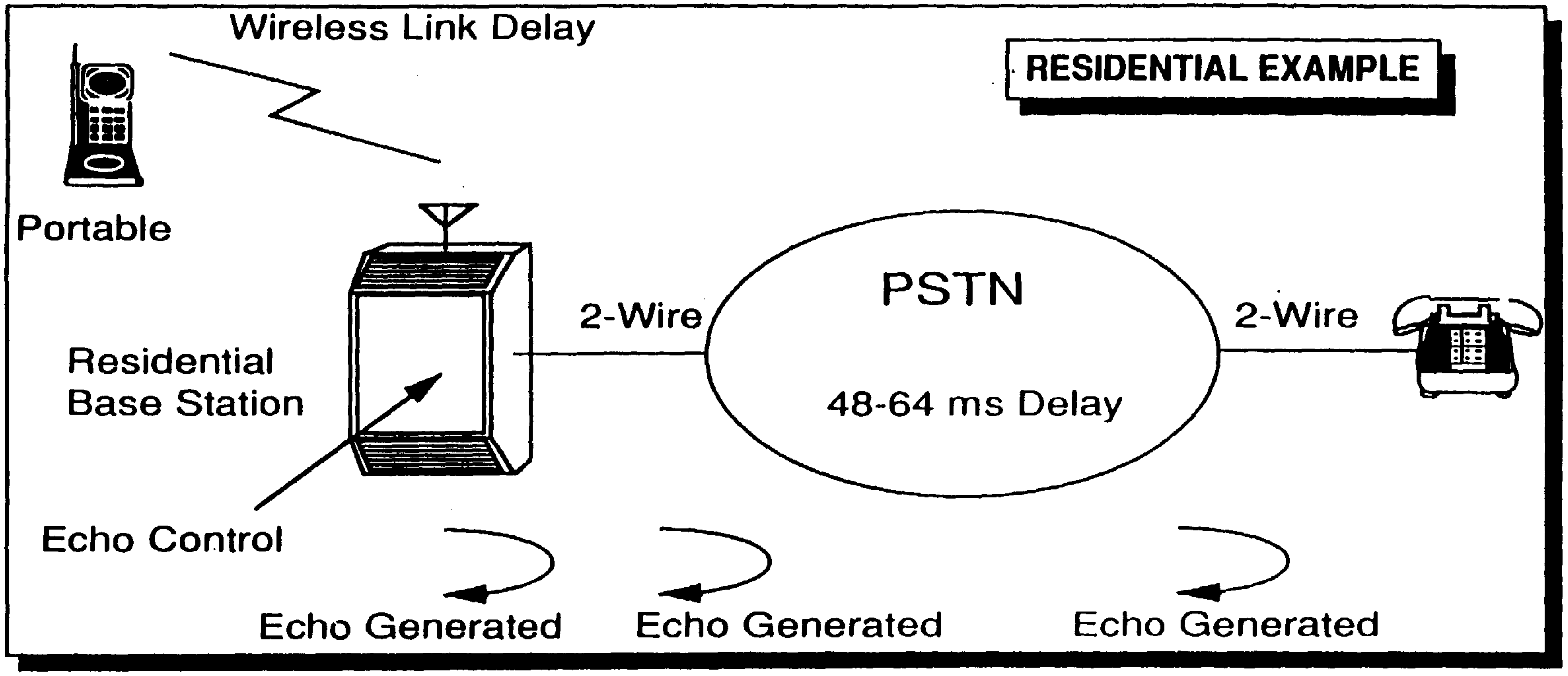
SYN=SYNCP

ID_OK

PID, LID, LS=10

(START LAYER 3)

PCI: Low Link Delay

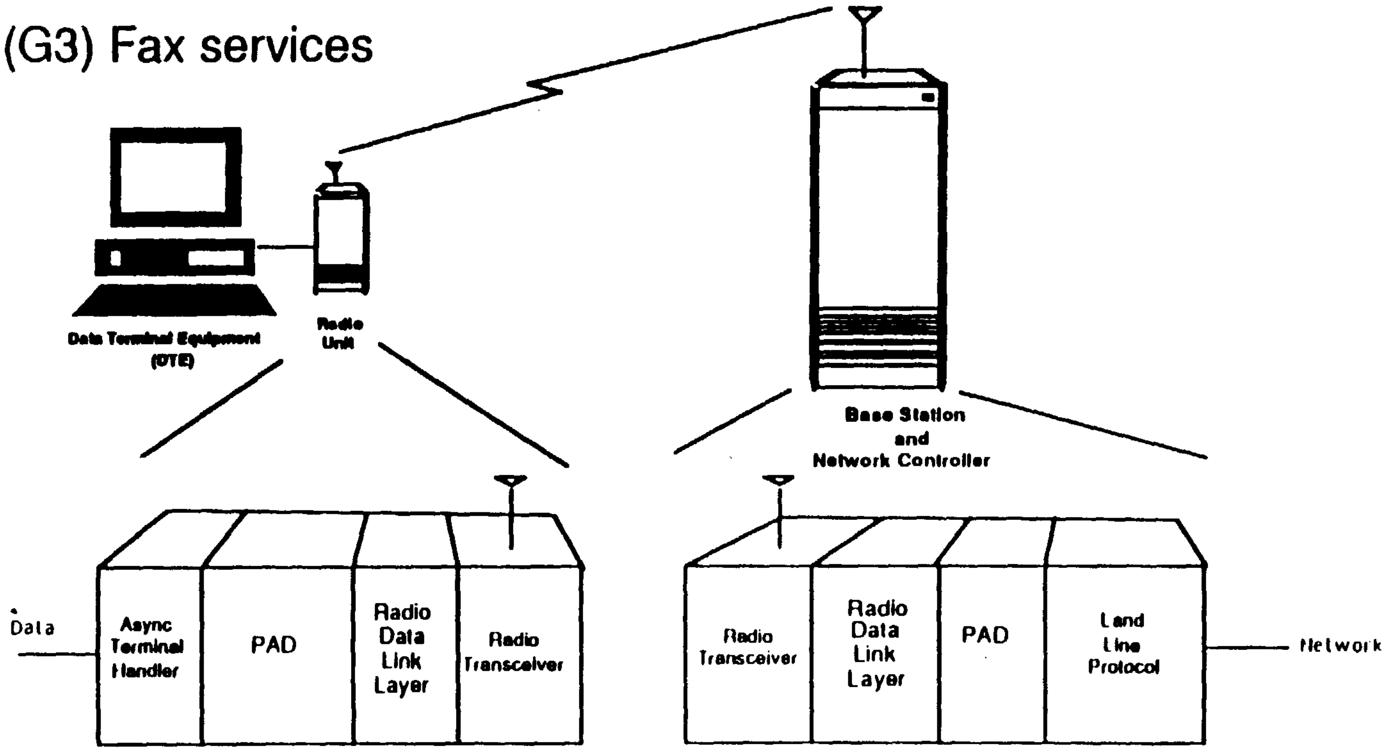


- An issue on PSTN connections
- Talker-echo performance degrades as delay increases; eventually, echo control measures become required
- Echo control measures necessitated by wireless link delay will have to be implemented at the subscriber end, adding to equipment cost

PCI Data Services

Multiple data services are supported over the 32 kbit/s B channel:

- full-duplex asynchronous data services
- transparent data services
- X.25 packet data services
- Group III (G3) Fax services



- PAD - Packet Assembler/Disassembler
- RDLL - Radio Data Link Layer
- LPL - Land-Line Physical Layer.

- V.32 modem (9600/4800 bit/s)
- V.22 bis modem (2400/1200 bit/s)
- V.21 modem (300 bit/s)
- Bell 212A modem (1200/300 bit/s)